論文審査の要旨および学識確認結果

報告番号	㊙／乙第　　号	氏　名	加藤　広野

論文審査担当者：				
	主査	慶應義塾大学教授	工学博士	笹瀬　巌
	副査	慶應義塾大学教授	工学博士	山中　直明
		慶應義塾大学教授	博士（工学）	大槻　知明
		慶應義塾大学教授	工学博士	池原　雅章

(論文審査の要旨)

工学士，修士（工学）,加藤広野君提出の学位請求論文は，「A Study on Machine Learning Based Detection of Android Malware and Stego Images（機械学習に基づいたAndroidマルウェアとステゴ画像の検知に関する研究)」と題し，全6章から構成される.

インターネット技術の向上に伴い，非常に便利な生活が実現しつつある一方で，電子ファイルやスマートフォンアプリなどのデジタルメディアを悪用した攻撃が,重大なサイバーセキュリティ脅威となっている．ウイルス対策ソフトにより，既知の攻撃に対する検知はなされているが，多様化した全ての脅威に対処できるわけではない.攻撃の存在を確認することにより，攻撃内容の分析や対処方法の検討が可能となるため，デジタルメディアにおける攻撃検知は，サイバーセキュリティ分野において，最も重要な研究領域の一つになっている．攻撃検知技術は，適用する場面によって，検知の対象や扱うことが可能なデータ形式等が大きく異なるため，それぞれに特化した対応策を講じることが喫緊の課題となっている.

本論文では，利用者や被害の多さの観点から，Androidマルウェアと，画像に悪性プログラムなどを人間の目には知覚できない微細なシグナルとして埋め込み，密かに攻撃を行うことが可能なステゴ画像に注目し，これらに対して，機械学習に基づいた効率的な検知方式を提案し，データ分析や計算機シミュレーションにより，提案方式の有効性を示している.

第1章では，デジタルメディアにおけるサイバーセキュリティ脅威と攻撃検知の重要性，および，当該技術が用いられる領域を概観し，本研究の目的と位置付けを述べている.

第2章では，システムモデルと攻撃者モデルの定義を行なったのち，本研究に関連する従来研究について述べ，実データセットの分析を通して，それらの問題点を明らかにしている.

第3章では，SSL（Secure Sockets Layer）サーバ証明書の認証レベルに着目した．Androidマルウェア検知法を提案している.実データセットを用いた評価を行い，提案方式は，従来方式が検知できないマルウェアを検知し，検知精度が向上することを示している.

第4章では，パーミッションペアの構成比に着目した，Androidマルウェア検知法を提案している．実データセットを用いた評価を行い，提案方式は従来方式と比較して，検知結果の解釈を容易にし，学習時間および検知精度に関して優れていることを示し,実運用に適していることを明らかにしている.

第5章では，シグナル埋め込み前に縮小リサイズが施されたステゴ画像への対策として,近年のシグナルの埋め込み手法では，画像に複数回適用した場合は連続して同様の箇所に埋め込む傾向があることに着目し，シグナルを強調して学習を促進する検知方式を提案している．実データセットを用いたシミュレーションを行い，提案方式は従来方式と比較して，縮小リサイズ後に作成されたステゴ画像の検知精度を向上できることを示している.

第6章は結論であり,本論文の内容および今後の課題を総括している.

以上，本論文の著者は，デジタルメディアにおける脅威であるAndroidマルウェアとステゴ画像に対して,機械学習に基づいた効率的な検知方式を提案し,データ分析や計算機シミュレーションにより,提案方式の有効性を明らかにしており，工学上，工業上寄与するところが少なくない．よって，本論文の著者は博士(工学)の学位を受ける資格があるものと認める.

学識確認結果	学位請求論文を中心にして関連学術について上記審査会委員で試問を行い，当該学術に関し広く深い学識を有することを確認した. また，語学（英語）についても十分な学力を有することを確認した.